IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

REYNALDO REYES, on behalf of himself and all others similarly situated, Plaintiff, v. ZIONS FIRST NATIONAL BANK, NETDEPOSIT, LLC, MP TECHNOLOGIES d/b/a MODERN PAYMENTS, TELEDRAFT, INC., NATIONAL PENN BANK, WELLS FARGO BANK, N.A., and WACHOVIA BANK, N.A., Defendants.	CIVIL ACTION NO. 10-00345 JURY TRIAL DEMANDED

CORRECTED DECLARATION OF PROFESSOR AMELIA BOSS IN SUPPORT OF PLAINTIFF'S MOTION FOR CLASS CERTIFICATION

1. I have been asked, as an expert in banking, and payment systems, to opine on the underlying conduct related to this action. In particular, I have been asked to (a) describe the operation of the ACH system as it relates to this case, explaining the relationships between the various parties and the manner in which ACH entries are processed; (b) describe in particular the types of ACH transactions that are at the heart of the present action (the TEL and WEB functions); (c) analyze the risks inherent in these types of ACH entries; (d) opine as to the proper procedures to be followed by banks in these types of transactions to minimize risks to all participants; (e) opine as to whether defendant Zions followed those procedures; (f) opine as to whether, based on the facts to date, defendant Zions knew the nature of fraudulent activity being carried out by the other defendants in this case; and (g) opine as to whether such knowledge can be proven by evidence common to all the class members.

2. In this engagement, I am being compensated $475.00 per hour for my time. I have consulted on numerous matters in the past, particularly in the payments areas. I have testified as an expert in one case in the preceding four years: *Robert J. Lewis v. Pertigallo, Bosick and Gordon LL.C.* (Pa. Ct. of Common Pleas, Allegheny County, Civil Division G.D. 06-016521). I testified specifically on fraudulent processing of payments before the Honorable Timothy Rice in the case of *United States v. Payment Processing Center LLC*, F. Supp. 2d 319, 3221-22 (E.D. Pa. 2006). (Civil Action No. 06-725(JP)), where my opinion was favorably received.

3. I was retained in this matter on September 21, 2012, and this declaration represents my analysis of this case to date. I reserve the right to supplement my opinion based on further factual discovery as this matter develops.

Credentials

4. My credentials are set forth in my attached curriculum vitae. However, certain aspects of my prior experience bear elaboration.

5. I am the Trustee Professor of Law at the Earle Mack School of Law at Drexel University, and have been teaching banking and payments systems for over twenty years. All of my research and scholarship focus on commercial practices (including payments systems banking practices) and law. I served on the Members Consultative Committee of the American Law Institute on the most recent changes to the Uniform Commercial Code (UCC) Articles 3 and 4, which set out a uniform set of state law rules governing the check payments. Since 1991, I have served on the Permanent Editorial Board (PEB) of the Uniform Commercial Code (and its Executive Subcommittee). The PEB and its members are charged, inter alia, with monitoring all developments in areas affected by the UCC, suggesting initiation of UCC revision projects where applicable, reviewing all proposed revisions, and (where appropriate), drafting Official PEB Commentary explaining the intended application and impact of Code provisions. That body also works closely with representatives of the Federal Reserve Banks to assure, to the extent possible, coordination between federal law and the uniform state law governing check and electronic funds payment systems. In my capacity as a member of the PEB (as well as a member of the Council of the American Law Institute, one of the sponsors of the UCC), I have also been a participant in the on-going discussions of the propriety of uniform legislation in the broader payments field.

6. I am past Chair of the American Bar Association's Business Law Section and its Uniform Commercial Code (UCC) Committee. The UCC Committee of the

ABA, through its Payments Subcommittee (of which I am also a member) closely monitors developments in the field of payments and works with industry and government on improving the legal structures in the field.

7. I am also a member of the Council of the American Law Institute (ALI), the governing body of one of the sponsors of the UCC. The Council is charged with overseeing all ALI projects such as the Uniform Commercial Code and must approve all proposals for change. I have participated in the drafting of revisions to Articles 1 (General Provisions), 2 (Sales), 2A (Leasing), 5 (Letters of Credit), 7 (Documents of Title), 8 (Securities), and 9 (Secured Transactions).

8. In all of these endeavors, the focus of my work has been on the evolution and accommodation of business and banking practices in the regulatory environment, and in that context I also consult with attorneys for businesses and financial institutions on evolving payment practices.

Materials Reviewed

9. In preparation for this case, I have reviewed the following materials:

- Amended Class Action Complaint, *Reynaldo Reyes v. Zions First National Bank* (E.D.Pa. No. 10-00345)

- Plaintiff's Memorandum in Support of Their Motion for Certification of This Action as a Class Action, *Mary Faloney v. Wachovia Bank* (E.D.Pa. No. 07 CC 1455 JP)

- Plaintiff's RICO Case Statement, *Reynaldo Reyes v. Zions First National Bank* (E.D.Pa. No. 10-00345)

- Motion for Summary Judgment against the NHS/PHS Defendants, *Federal Trade Commission v. NHS Systems, Inc.* (E.D.Pa. Civ. Action No. 08-cv-2215)

- Other documents and depositions produced in this case and cited below.

Overview of the ACH System

10. The ACH or "automated clearing house" system is a computer-based nationwide counterpart to the check system. It is a batch processing electronic payment mechanism, supporting both debit and credit transfers under which transactions (also called "entries") are processed in groups (batches) and released to the automated clearing house one or two days before the anticipated transfer is to occur. As all the entries involved in this case are consumer debit entries, I will limit my comments to those types.

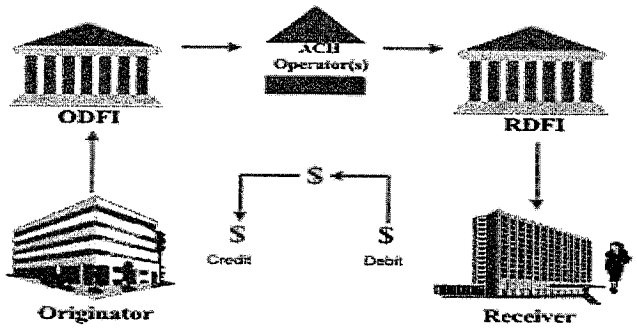
11. The end user participants in an ACH consumer debit transaction are the Originator, generally a merchant, whose account is being credited, and the consumer Receiver, whose account is being debited. The Originator initiates the transfer by instructing its own bank, the Originator's Depositary Financial Institution (ODFI) (the merchant's bank), to credit its account and debit the account of the consumer Receiver. The ODFI in turn relays the instruction (called an ACH "entry) to the ACH Operator(s),[1] who in turn routes it to the Receivers' Depositary Financial Institution (RDFI) (the consumer's bank), who then debits the account of the consumer Receiver.

12. In a debit transfer, the Originator sends a message to "debit the receiver" and has the amount credited to the Originator's account. In essence, the Originator is

[1] The two major ACH Operators in the United States are the Federal Reserve System, and the Electronic Payments Network in New York. Both processed payments in this case.

"pulling" the money from the Receiver's account. A common example of the debit transfer is when a credit card, utility or mortgage company is authorized by its customer to debit her checking account each month for the amount due.

13. The following diagram illustrates the relationship of the parties and the information flow in a consumer debit transaction.



14. In nearly all instances in this case, defendant Zions was the ODFI responsible for introducing the debit entries into the ACH system. The originators were the various telemarketers.[2] Modern Payments, NetDeposit and Teledraft each served as what is known as a "Third-Party Sender," also referred to as a "Third-Party Service Provider" or "Third-Party Payment Processor," an entity performing ACH entry processing functions who acts as an intermediary between the Originator and the ODFI. The following diagram illustrates the relationship between the parties when a Third-Party Sender is involved:[3]

[2] "Telemarketers," when used in the context of the entities involved in this case, refers to each of the following: The NHS/PHS group, Vexeldale and its related entities; Group One and its related entities; Low Pay; the Platinum Benefit Group; and Rxsmart.

[3] NACHA, Third-Party Sender Case Studies: ODFI Best Practices to Close the Gap: An ACH Risk Management White Paper (2009).

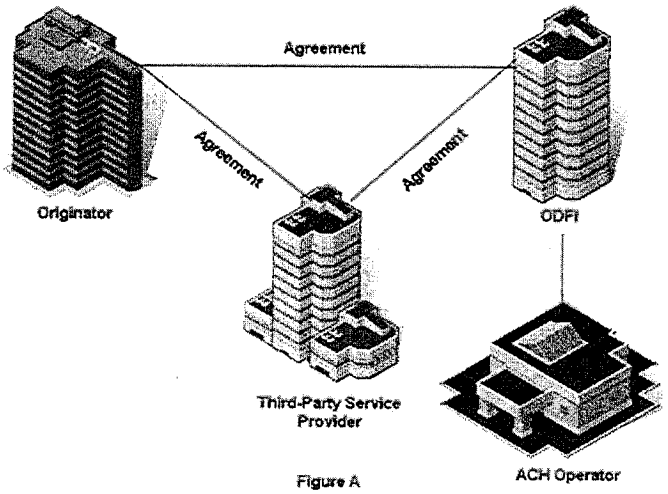


Figure A

While the diagram above demonstrates the normal relationship between the parties, in this case there were no specific agreements executed between the ODFI (Zions) and either of the Third-Party Senders (Modern Payments and NetDeposit) or between the ODFI (Zions) and any of the telemarketer Originators.

Governing Law

15. Transmission of debit and credit entries and entry of data over the ACH network is governed by the NACHA Operating Rules ("2008 Operating Rules"), as supplemented and amplified (but not superseded) by the NACHA Operating Guidelines ("2008 Operating Guidelines.") NACHA (formerly the "National Automated Clearing House Association") is a non-profit membership association of over 10,000 members that manages the development, administration, and governance of the ACH Network and all participants using the system.

16. In addition, the Electronic Funds Transfers Act, 15 U.S.C. § 1693 et seq., and its implementing Regulation E, 12 C.F.R. § 205, may apply to some parts of the

transfers into or from a consumer account, while Uniform Commercial Code Article 4A governs certain non-consumer entries. Furthermore, while debit transactions resemble the processing of the checks but are not technically within the coverage of UCC Article 4, ACH Rule 14.1.28 deems Article 4 to apply to these transactions in a way not relevant to the issues in this case.

17. Lastly, the general regulatory structure within which banks operate, including the Bank Secrecy Act (BSA) and regulations of the Office of the Comptroller of the Currency (OCC), apply and impose, among other things, monitoring obligations upon governed financial institutions.

ACH Debit Entries

18. There are a number of different types of ACH transactions or entries. The relevant applications for the purposes of this case include the following entry types:

- PPD (Prearranged Payment and Deposit Entry): This entry is to credit or debit a consumer account as prearranged between the Originator and the Receiver. It is popularly used for payroll direct deposits and preauthorized bill payments. In a PPD, the authorization given by the consumer must be in writing and signed or similarly authenticated by the consumer authorizing repeated debits by the originator, and the consumer must be provided with an electronic or paper copy of the authorization;

- WEB (Web-Initiated Entry): Electronic authorization is obtained through the Internet to create an ACH entry. As discussed below, there are restrictions placed on when the WEB entry may be used; and

- TEL (Telephone-Initiated Entry): Oral authorization is obtained from the customer by telephone to issue an ACH entry. As discussed below, there are significant restrictions placed on when the TEL entry may be used. TEL entries may not be used for outbound telemarketing.

Risks of Fraud in the ACH System: Who Has the Keys

19. At the outset of electronic banking, ACH payments consisted of preauthorized arrangements between payors and payees who were familiar with one another, and the payments occurred in a sustained and systematically recurring manner (for example, automatic deposit of payroll salaries and the pre-authorized monthly payment of an insurance premium or mortgage) with the verifiable written approval of the customers involved. These are the types of transactions that would fall into the PPD code mentioned above.

20. A foundation of the ACH system is that the main (and only) point of entry into the system is a bank. The ACH system was built on the concept that all ACH entries would flow into the ACH processing system through a bank – the ODFI or Originator's Depositary Financial Institution – that would ensure the integrity of the transfers made.

21. While entry to the ACH system is through the ODFI, the instructions themselves originate with the Originator. In the past, an Originator wishing to set up recurring entries to a consumer's account had to obtain, in advance and in writing, authorization which was then provided to the bank before any entries could be initiated.

22. Over the past decade or so, new applications have emerged – what are often called "electronic checks" or "e-checks" – which are not pre-authorized in advance.

More importantly, they are relatively anonymous and are frequently characterized by the lack of an established relationship between the payee merchant and the consumer payor, and are often on a one-time, non-recurring basis. Moreover, as the ACH network has evolved into a general-purpose payments network, a new industry has grown up of Third-Party Processors or Third-Party Senders who often stand between the bank and the merchant originating the payment, aggregating ACH entries for processing.

23. These developments have increased the risk of fraudulent activity by those originating ACH debit transfers. All that an Originator or Third-Party Sender needs to obtain access to the ACH system (and to charge the accounts of consumers throughout the country) is the account numbers of potential victims and an Originating Institution, such as Zions, willing to process ACH entries on its behalf. Because of the way that debit or "pull" entries are initiated (by information provided by a merchant to the ODFI), the main check against potentially fraudulent activity is to police the entry into the system. In other words, the ODFI is in effect the "gateway" to the payment system. It is the only player in the ACH system in a position to assess the credibility and trustworthiness of the Originator that is the source of the entry, and is the one in the best place to prevent fraud and minimize loss.

24. For these reasons, the ODFI is responsible for all entries into the ACH system made under its routing number, regardless of the identity of the Originator or Third-Party Sender. Also, for these reasons, these new applications are subject to a number of requirements and limitations designed to safeguard the system against fraud.

25. To the limited extent that consumer transactions initiated and authorized over the telephone or internet are permitted in the ACH system, these ACH entries

present a higher risk of fraud than other ACH transactions. First, the ACH entries are initiated by the merchant, not the consumer, and the merchant in essence "reaches into" the consumer's account to have money transferred to its own account. Second, most other ACH entries require written authorization from the customer for the initiation of any debit entry. Where the transaction occurs over the telephone, the authorization is obtained verbally and is more prone to fraudulent overreaching. Over the internet, they are obtained electronically and are subject to falsification or interception. Third, the amounts involved in these transactions may be relatively small, reducing the likelihood that the victims will notice the fraud, and, if they do notice it, the likelihood that the victims will be able to spend the time, energy and resources required to deal with the merchant and the bank to get the entry reversed. Fraudsters rely on the fact that much of their fraudulent activity will go undetected, and they rely on numerous small dollar transactions which, when aggregated, may be very substantial.

26. It bears emphasizing that the failure to complain in such instances does not amount to express or verifiable authorization; the failure most often stems from failure to discover the fraud or the roadblocks encountered by a consumer who does discover the fraud. Many fraudulent schemes operate on the principle that with high volume, low dollar entries much of the fraud will go undetected by the victims (the Receivers) earning the fraudsters large sums in the aggregate.

Telemarketing Creates a High Risk of Fraud in the Payments Area.

27. The risk of fraud in telemarketing is well known in the payments area. In 1999, the Office of the Comptroller of the Currency warned banks of this risk in its manual for banks, *CHECK FRAUD: A GUIDE TO AVOIDING LOSSES* 93 (1999):

> The criminal calls a consumer and announces the consumer has won a prize. The criminal explains that, to deposit the prize into the winner's account, he or she needs the account information. Once the consumer provides the account information, the criminal prepares demand drafts and withdraws funds from the account. A common variant is for the criminal to offer the consumer something for sale, such as a magazine subscription, in order to get the necessary information.

28. While the manual refers to the use of demand drafts (or remotely created checks which are processed through the checking system rather than the ACH system), the same fraud is often perpetrated with the use of ACH payments. Indeed, the two payment mechanisms, an "RCC" entry in the checking system and an ACH entry, share an important characteristic: while the transaction results in the consumer's account being debited, the debit transaction is originated by the payee rather than the customer, using the customer's banking information, and the transaction proceeds on the assumption (an incorrect assumption in the event of fraud) that the consumer whose account is being debited has actually authorized the debit. At the point of origination, the process is the same: the telemarketer gets from the customer the customer's banking information (essentially the bank routing numbers appearing in the computer readable MCR code at the bottom of the check). It then either proceeds to "write a check" against that amount (a remotely created check) which is then presented to a customer's bank for payment, or it creates an ACH order – an ACH transaction in which the customer's bank account is debited and that of the telemarketer or its payment processor is credited. Credit cards are generally not used in such fraudulent telemarketing campaigns for multiple reasons: the right of the consumer to "charge back" in these settings is much greater, major credit card associations impose heavy fines on merchants whose chargeback rate is over 2 ½ percent, and credit card companies have been vigilant in instituting fraud detection mechanisms aimed at such activity. For a discussion of remotely created checks in instances of

telemarketer fraud. *See United States v. Payment Processing Ctr.*, 461 F. Supp 2d 319, 321-22 (E.D. Pa. 2006).

29. I understand that the defendants in this action have sought to distinguish the Payment Processing Center action and subsequent action against Wachovia Bank from this case because they involved RCC transactions. As should be clear from the above and from what follows, there is no relevant distinction with regard to the issues of a bank's involvement in fraud. Rather, anything said or found regarding a bank's conduct with regard to RCCs should apply with greater force to ACH transactions. That is because ACH transactions are subject to greater regulation and capable of much closer scrutiny.

30. Because of the substantial risk of fraud in telephone initiated transactions, NACHA places stringent limitations on the ability of Originators to use the TEL entry (the entry designed for telephone initiated ACH debits), as will be discussed below. Yet these limitations on TEL entries do not provide absolute protection: Originators or Third-Party Senders may improperly code the transaction to mask its true nature, or may ignore the limitations placed on TEL and other entries. The ODFI, however, when it transmits the entry, warrants that each entry it transmits is in accordance with the proper authorization provided by the Originator and the Receiver. NACHA 2008 Operating Rules 2.2.1.1.

31. Telemarketers have long been identified as "high-risk customers." They increase the risk of fraud in systems such as the ACH system, and require additional due diligence and close monitoring by the ODFIs doing business with these high risk

merchants. *See, e.g., 2000 Comptroller's Handbook*, at 33; OCC Bulletin 2006-39 (telemarketers "inherently more risky"); OCC Bulletin 2008-12.

Bank Fee Structures Create Negative Incentives to Police against Fraud in ACH transactions.

32. An ODFI that does business with fraudulent Originators can protect against risks to itself and at the same time increase its profitability. Banks can reassign their risk, and their exposure, to others (including the Third-Party Sender) by contract (using, in many cases, indemnity agreements) or they can require reserves. At the same time, they can increase profitability by charging high return rate fees that earn them more fees as returns increase. In so doing, however, the banks risk perpetuating fraud against innocent parties (the customers) who do not have such ability.

33. The existence of these negative incentives has been recognized by the Office of the Comptroller of the Currency. Karen Furst and Daniel Nolle, *What's Your Risk with the Growing Use of ACH Payments? QUARTERLY JOURNAL, OFFICE OF THE COMPTROLLER OF THE CURRENCY*, Vol. 24, No. 4 (2005), at 35:

> [G]rowth in return items is likely to exacerbate potentially unsafe and unsound incentives embedded in the ACH returns system. In particular, fee income from return items can become an important source of non-interest income for an originating bank. Even if an ACH transaction originator (i.e., the payee) has an unusually high level of returns, from a fee perspective, the bank for whom that originator is a client has a disincentive to deny or even limit ACH origination services, because the bank earns a fee from the originator on both the initial presentment of the (faulty) debit entry, as well as the return. Additionally, and unlike in the case of check-processing, a bank originating ACH debit transactions is not constrained by the necessity of having to maintain demand deposit accounts with every originator. Under these circumstances, some banks may not scrutinize returns at the originator level, increasing the likelihood that they will continue to process transactions for acquired merchants with high return rates operating through one or more Third-Party Senders.

34. This type of fraud causes damages to the system (including not only out-of-pocket costs incurred by the handling of the forward and return items but reputational costs as well) and to the victims. Victims incur out-of-pocket losses from their account, returned check fees, bounced check fees, time and associated loss of reputation, etc. Many victims are ignorant of the fraud or unaware of the remedies they have; others encounter such roadblocks that they drop efforts to seek redress.

Banking Regulations and Practices Require ODFI Action to Combat Fraud and Other Illegal Activity Through the Underwriting of New Customers

35. Banks are required by statute (including the Bank Secrecy Act, 31 U.S.C. § 5311 et seq.,) and regulation (*see, e.g.*, 31 C.F.R. § 103) to institute and implement detailed compliance programs aimed at preventing illegal use of the banking system. The Office of the Comptroller of the Currency (OCC) and the Federal Financial Institutions Examination Council (FFIEC), which includes the OCC and other bank regulators, have spelled out these requirements in detail in a series of handbooks and examination manuals. These documents provide that, as the gatekeepers and points of entry to the ACH system, ODFIs have a special obligation to guard against fraudulent behavior. The ODFI's responsibilities include the development of internal policies and procedures to guard against risk, the exercise of due diligence and underwriting in the "on-boarding" or acceptance of a new customer), and the continued monitoring of their participation in the ACH system, including monitoring payments processed and corresponding return rates.

36. First, a bank is required to establish policies and procedures to guard against the risk of fraudulent activity. Those policies and procedures must include the identification of high risk banking operations (which may include electronic funds

transfers); risk-based customer due diligence; sufficient controls and monitoring systems for the timely detection and reporting of suspicious activity policies, procedures, and processes; and appropriate training and supervision of employees. *See FFIEC BANK SECRECY ACT / ANTI-MONEY LAUNDERING EXAMINATION MANUAL* (2007) ("2007 BSA/AMLA MANUAL"). The FFIEC has identified certain products and services that facilitate a higher degree of anonymity while involving high volumes of currency, thereby creating a higher risk of money laundering or terrorist financing; included in that list are electronic funds payments services, including third party processors and ACH transactions. 2007 BSA/AMLA MANUAL 20.

37. As part of those policies:

> One of the most important, if not the most important, means by which financial institutions can hope to avoid criminal exposure to the institution by "customers" who use the resources of the institution for illicit purposes is to have a clear and concise understanding of the "customers'" practices.

Bank Secrecy Act Manual 601.0 (Board of Governors of the Federal Reserve Board, Sept. 1997). The "Customer Due Diligence" or "Know Your Customer" procedures are the underwriting necessary in "on-boarding" or taking on new customers.

- Each bank is to have a customer profile allowing it "to understand all facets of the customer's intended relationship with the institution, and, realistically, determine when transactions are suspicious or potentially illegal." *Bank Secrecy Act Manual* 601.0 (Board of Governors of the Federal Reserve Board, Sept. 1997).

- Banks are required to institute CDD programs designed "to enable the bank to predict with *relative certainty* the types of transactions in which a customer is likely to engage." *Id.* (emphasis added); *Bank Secrecy Act/Anti-Money Laundering Examiner's Manual*, 37 (FFIEC, 2006); *2007 BSA/AMLA MANUAL* at 56.

- Banks are required to institute "enhanced due diligence" for "high-risk customers." *2007 BSA/AMLA MANUAL* at 57. "High-risk customers and their transactions should be reviewed more closely at account opening and more frequently throughout the term of their relationship with the bank." *Id.*

38. In the underwriting of new customers, particular care should be taken in the case of "high risk" customers. In 2006, The Office of the Comptroller of the Currency stressed that ACH transactions involving certain high-risk originators (including telemarketers) or that involve third-party senders face increased reputation, credit, transaction, and compliance risks. *Automated Clearing House Activities: Risk Management Guidance*, OCC Bulletin 2006-39. Furthermore, it observed that high-risk originators, including companies often engaged in potentially illegal activities or with an unusually high volume of unauthorized returns, frequently utilize the services of a Third-Party Sender because they have difficulty establishing a relationship directly with a bank. Thus the OCC cautioned that before a bank engages in high-risk ACH activities, the board of directors should consider carefully the risks associated with these activities and either prohibit transactions with certain high-risk originators and Third-Party Senders or provide guidance on the parameters within which such activities are to be carried out.

39. In 2006 and again in 2008 and 2009, the OCC published guidance on how a bank should handle risks of fraud in the ACH system. The 2006 OCC Bulletin 2006-39 identified the area of Bank Underwriting Standards (applied before new customers or originators are allowed to initiate ACH entries) as critical. The advice noted that all ODFIs should adopt a formal underwriting and an approval policy for ACH Originators, and reject originators with a history of excessive unauthorized returns, or those that do not operate a legitimate business. The underwriting standards should:

- Define desirable, prohibited and restricted originators;
- Require background checks on the legitimacy of the originator's business;
- Require evaluation of the originator's creditworthiness;
- Require review of the originator's sales history;
- Provide authorization procedures for approved originators;
- Provide guidelines for exposure limits;
- Establish over-limit monitoring and approval;
- Outline originator account termination procedures;
- Allow the bank to audit originators' ACH processes and controls.

40. When a Third-Party Sender is involved, the due diligence and underwriting that is required of the ODFI is not limited to the Third-Party Sender, but extends to the Originators who are the customers of the Third-Party Sender. The OCC's statement is clear: "banks should require Third-Party Senders to provide certain information on their Originator customers such as the Originator's name, taxpayer

identification number, principal business activity, and geographic location. Also, before originating transactions, a bank should verify that the Originator is operating a legitimate business." *Automated Clearing House Activities: Risk Management Guidance*, OCC Bulletin 2006-39.

NACHA Regulations and Practices Require ODFI Action to Combat Fraud and Other Illegal Activity in the ACH System

41. The NACHA network and its governing Rules and Guidelines impose limitations designed to minimize and eliminate fraud in ACH processing. In 2002, NACHA adopted the following policy statement:

> The NACHA Board believes that the Automated Clearing House Network must maintain the highest standards of fraud prevention to retain the integrity of the payment mechanism and the trust and confidence of its users. Therefore, the NACHA Board resolves and strongly urges that all participants implement adequate control systems to detect and prevent abusive fraud and abusive financial transactions.

2008 NACHA Operating Rules and Guidelines xvii.

42. More specifically, NACHA in its Operating Rules places limits on the use of the system in the following manner, among other things:

- An ODFI that deals with a Third-Party Sender must enter into an appropriate agreement under which the Third-Party Sender agrees to be bound by the NACHA rules, agrees only to use the system for lawful purposes, and agrees to assume the responsibilities of an Originator. 2008 Operating Rule 2.1

- Any consumer receiver whose account is to be debited must provide authorization in a writing signed or similarly authenticated by the consumer. Detailed rules govern this authorization requirement. 2008 Operating Rule 2.1.2

- In the case of TEL transactions, the authorization may be oral, but it must be readily identifiable as an authorization, must clearly state its terms, and must include certain required information. 2008 Operating Rules 2.1.8

- More importantly, the use of TEL entries is limited; the use of TEL transactions for outbound telemarketing is prohibited, as is the use of TEL for recurring debits. 2008 Operating Rules 14.1.63.

- An ODFI sending an ACH entry warrants that the entry has been properly authorized by the consumer receiver (as well as the Originator), 2008 Operating Rules 2.2.1, and that the authorization has not been revoked. 2008 Operating Rules 2.1.1.4. Breach of warranty leaves the ODFI open to liability for breach of warranty. 2008 Operating Rules 2.2.3.

43. Specific codes carry additional limitations and responsibilities. In the case of WEB entries (initiated on the internet) and TEL entries, the ODFI warrants that the Originator submitting the entry has employed commercially reasonable methods of authentication to verify the identity of the receiver. 2008 Operating Rules 2.11.2.2; 2.13.2.1. In the case of the PPD code, the ODFI warrants that there is a pre-existing, written authorization by the receiver. 2.1.2

44. The choice of which ACH entry to use is determined by how the authorization to initiate the entry was obtained. In most cases, this is based solely on a representation by the Originator to its bank, the ODFI. This puts the responsibility on banks to assure that the correct coding is used, as an ODFI warrants that each entry it transmits is in accordance with proper authorization provided by the Originator and the Receiver. 2008 Operating Rules 2.2.1.1.

45. In the case of ACH entries sent by a Third-Party Sender, the ODFI warrants that it has established procedures, on an on-going basis, to monitor the credit-worthiness of the Originator or Third-Party Sender, has established an exposure limit for the Originator or Third-Party Sender, has implemented procedures to review the exposure limit periodically, and has implemented procedures to monitor entries sent by the Originator or Third-Party Sender. 2008 Operating Rules 2.1.12.

46. The risk of fraud in ACH TEL entries has also led NACHA to enact rules (the TEL rules) restricting the use of the TEL entry in telemarketing. It specifically prohibits the use of the ACH system for telemarketing payments initiated by outbound telemarketing. 2008 Operating Rule 14.1.63 provides that TEL entries may be used only if the Receiver: (1) has initiated the telephone call; or (2) there is an "Existing Relationship" between the Receiver and the Originator.

47. An "Existing Relationship" exists under 2008 Operating Rule 14.1.30 for TEL entries if there is a written agreement between the Receiver and the Originator or the Receiver has purchased goods or services from the Originator within the past two years.

48. TEL entries are allowed only for "Single Entry" transfers. A Single Entry transfer under 2008 Operating Rule 14.1.67 is a one-time transfer initiated by an Originator in accordance with the Receiver's authorization for a single ACH debit or credit to the Receiver's consumer account. Moreover, a TEL (at the time of the events involved in this case) could not be used for recurring payments (even though they do not involve outbound marketing); consequently under the NACHA rules, recurring payments fall under the general rule that requires, in the case of consumer debits, that the authorization be in a writing signed or similarly authenticated. 2008 Operating Rules

2.1.2. Recurring entries would typically fall under the PPD (Prearranged Payment or Deposit), yet that SEC code cannot be used for an entry initiated telephonically. Thus, there is no way to transmit a recurring debit authorized telephonically within the ACH system.

49. NACHA recognizes the correlation between high return rates and fraud and in the context of TEL entries in particular and has established TEL entry reporting requirements. Under NACHA's Entry Reporting Requirements, if NACHA believes that the return rate for TEL entries that are returned as unauthorized for any Originator may exceed 2.5% (later lowered to 1%), NACHA may request the ODFI to provide information with respect to the returns of that Originator. 2008 Operating Rules 2.13.3. If the ODFI fails to provide the information within ten banking days of the receipt of the request, the failure will be considered a "willful disregard" of the ACH Rules and subject the ODFI to the imposition of a fine as provided in Appendix 11 to the 2008 Operating Rules.

50. It should be noted that while the NACHA rules lacked significant sanctions and other enforcement mechanisms prior to the 2008 amendments, the rules imposed very clear reporting requirements on ODFIs with high rates of return of TEL transactions. The rule establishing a 2.5% threshold for that reporting requirement should not be read to sanction or condone rates *below* the 2.5% figure. According to both the OCC and NACHA guidelines, a 2.5% return rate is "well above the acceptable rate for normal business purposes." 2008 NACHA Operating Guidelines 245; OCC Bulletin 2006-39.

51. On September 19, 2002, NACHA issued an Operations Bulletin specifically addressing the fraud risk inherent in TEL entries, identifying the risk management concerns and the obligations of the ODFI related to authorization and use of the TEL entry. *NACHA Rulemaking Process Operations Bulletin, Telephone-Initiated (TEL) Entries* (Sept. 19, 2002). The Operations Bulletin noted that telemarketers, who frequently use TEL entries to process payment, often misuse the TEL entry and engage in unfair and deceptive trade practices. Those practices include acting with fraudulent intent to debit consumer accounts without authorization; cold-calling customers with whom they have no previous relationship and manipulating the TEL rules by using mail solicitations to induce customers to initiate the call to the telemarketer and then selling their wares with deceptive practices.

52. The 2002 Operations Bulletin stressed the critical role played by ODFIs:

> It is critical that ODFIs understand that, under the NACHA Operating Rules, they are responsible for all transactions initiated into the ACH Network. To that end, they must recognize that they will be exposed to substantial risk when offering origination services on behalf of merchants that are engaged in fraudulent or deceptive business practices.

53. The 2002 Operations Bulletin proceeded to lay out steps ODFIs should take to minimize the risk of loss:

- ODFIs must take steps to ensure that they know their customers and are familiar with their business practices;

- In any situation where the ODFI's customer is a third-party service provider, the ODFI must ensure that it has entered into contractual agreements with the ultimate Originators of the transactions and that it is familiar with the

business practices and risks associated with originating entries on behalf of each individual Originator; and

- ODFIs should understand that offering direct access to the ACH Operator adds risk to the ODFI. The ODFI remains responsible for all transactions originated under its routing number but may have no knowledge of the types or dollar values of payments being originated. ODFIs must ensure that they have established monitoring capabilities to examine entries entered into the ACH Network under its routing number and to restrict the origination of any files that seem questionable.

Banking Regulations and Practices Require Additional ODFI Action to Combat Fraud and Other Illegal Activity When a Third-Party Sender is Involved

54. Over the years, the payments industry has seen the growth of non-bank parties known as Third-Party Senders (or Third-Party Payment Processors), whose function is to accept various types of payments (RCCs, ACHs, etc.) from merchants, consolidate those payments, and in turn submit them for processing. The imposition of such a middle person increases the risk of fraud because of the separation of the ODFI from the entity initiating debit transaction. This increases the need for banks to be vigilant and monitor against fraudulent activity. The 2006 OCC Bulletin 2006-39 noted that high-risk originators including companies engaged in potentially illegal activity or those with an unusually high volume of unauthorized returns "often initiate transactions through third-party senders because they have difficulty establishing a relationship directly with a bank." In instances where Third-Party Senders are interposed between the merchant Originators and the ODFI, the ODFI undertakes additional responsibilities in

the underwriting context to assure that it is not allowing access to the ACH system by persons engaged in illegal activity.

55. In their BANK SECRECY/ANTI -MONEY LAUNDERING EXAMINATION MANUAL (2006) the Federal Reserve and the Office of the Comptroller of the Currency warn that "If a bank has not implemented an adequate processor-approval program that goes beyond credit risk management, it could be vulnerable to money laundering, identify theft, and fraud schemes." (205-206). It further warns that "some processors may be vulnerable to money laundering, identity theft, and fraud schemes." (108-109). The manual includes the following advice to banks: understand the payment processors' merchant base and the merchant's activities, and monitor the "charge-back history", i.e. the number of returned items from other banks.

56. OCC Bulletin 2006-39 (September 1, 2006), dealing with ACH activities, contains a section separately dealing with "Third-Party Senders" which requires that "Banks that initiate ACH transactions for third-party senders should know at a minimum, for which originators they are initiating entries into the ACH network. Thus, banks should require third-party senders to provide information on their originator customers such as the originator's name … principal business activity, and geographic location. Also, before originating transactions, a bank should verify (directly or through a third-party sender) that the originator is operating a legitimate business."

57. The NACHA rules recognize the risks inherent in the use of Third-Party Service Providers. Under Article 5, the Third-Party Sender is obliged to respond to requests for information by the ODFI (2008 Operating Rules 5.1), warrants that the Originator has agreed to assume the responsibilities of the Originator (2008 Operating

Rule 5.2), and indemnifies the ODFI from and against claims and losses resulting from the failure of the Originator to perform its obligations (2008 Operating Rule 5.2). The Third-Party Sender also assumes certain ODFI warranties and responsibilities (2008 Operating Rule 5.3), assumes certain Originator responsibilities (2008 Operating Rule 5.5), and agrees to pay the ODFI for any credit entries originated and any debit entries returned by the RDFI (2008 Operating Rule 5.4).

58. Furthermore, an ODFI receiving entries from a Third-Party Sender must establish exposure limits for that Third-Party, implement procedures for periodic review of that limit, and implement procedures to monitor those Third-Party Sender entries. 2008 Operating Rule 2.1.12.

59. NACHA rules also require the ODFI to have contractual agreements with Third-Party Senders specifying that the Third-Party Sender agrees to be bound by NACHA rules and applicable laws and regulations, and that entries may not be initiated that violate the laws of the United States. 2008 Operating Rule 2.1.1

60. The 2006 OCC Bulletin 2006-39 stressed the importance of "strong systems to monitor and control risk." "These systems should monitor the level of unauthorized returns, identify variances from established parameters such as origination volume, and periodically verify the appropriate use of SEC codes, as transactions are sometimes coded incorrectly to mask fraud."

61. In 2008, the OCC published OCC Bulletin 2008-12 specifically providing guidance to national banks for due diligence, underwriting, and monitoring of Third-Party Processors. This guidance summarized the existing procedures described above:

> When a bank has a relationship with a processor, it is exposed to risks that may not be present in relationships with other customers. The bank encounters strategic, credit, compliance, transaction and reputational risks in these relationships. Banks have two distinct areas of responsibility to control these risks. The first is due diligence and underwriting, and the second is monitoring these high-risk accounts for high levels of unauthorized returns and for suspicious or other unusual patterns of activity. Proper initial due diligence, effective underwriting, and ongoing account monitoring are critical for bank safety and soundness and consumer protection. Banks should implement these controls to reduce the likelihood of establishing or maintaining an inappropriate relationship with a processor through which unscrupulous merchants can gain access to consumers' accounts.

62. According to the OCC, banks must have a due diligence and underwriting policy that "among other things, requires an initial background check of the processor and its underlying merchants to support the validity of the processor's and the merchants' businesses, their creditworthiness and business practices." The OCC specifically noted that in the case of "higher-risk processors and merchants (e.g. telemarketers)" controls should be more rigorous. OCC Bulletin 2008-12.

63. The OCC also observed that banks needed to be "alert to processors' merchant clients that obtain personal account information inappropriately" to facilitate creation of unauthorized ACH entries. Controls include requiring the processor to provide information on its client, and verification by the bank that the merchant is operating a legitimate business. Verification should include checking public record databases, and fraud and bad check databases, and references from other financial institutions. OCC Bulletin 2008-12.

64. As for monitoring, the OCC noted that the bank's risk management program should include monitoring processor information such as merchant data, transaction history, and charge-back history. The bulletin noted that banks "should not

accept high levels of returns *regardless of the return reason.*" High levels of ACH debit returns are indications of fraud and "should not be accept[ed] . . . on the basis that the processor provided collateral or other security to the bank." OCC Bulletin 2008-12 (emphasis added).

65. ODFIs should be aware of the risks inherent in dealing with Third-Party senders, take adequate steps to know not only the business of these Third-Party senders but the Originators as well, monitor the activity of such senders, and either impose controls on Third-Party Senders or accept the fact that they may be facilitating fraud and abusive practices.

Monitoring of ACH Returns is a Critical Tool in ODFI Fraud Mitigation

66. A third, and critical, responsibility of an ODFI is to continually monitor its ACH operations, and in particular to monitor the extent and nature of items returned by receiving banks. The vast majority (almost 99%) of all debit transactions go through without a hitch, and the overwhelming percentage of banks never (or rarely) have debits returned as "unauthorized." Hence, the monitoring of return rates in ACH transactions is recognized as critical in ACH risk control. *See* Olivier Armantier, Michele Braun, Ron J. Feldman, Dennis Kuo, Mark Lueck, Richard M. Todd, *A Method for Improving the Benchmarks Used to Monitor ACH Returns*, Federal Reserve Bank of Minneapolis Financial Policy Working Paper (March 2010), at 6-7:

> Ex-post monitoring of return rates is an important part of the ACH risk control tool kit. It does not eliminate the need for controls such as careful due diligence before agreeing to process debits for a customer, but it has its own important role. Up-front due diligence is never perfect, and customers with no obvious initial risk factors may turn out to be problematic after a relationship has been initiated. Other controls,

> such as automated edits of transactions and diligent staff training, can mitigate risks that are already well-known, but they lag behind emerging types of fraud and error. Monitoring of customer returns by financial institutions is thus an essential backstop for spotting fraud when prevention fails and for identifying new types of fraud and nonfraud risks as they emerge. Without monitoring, a specific ACH customer might originate a large volume of unauthorized, possibly fraudulent consumer debits over an extended period of time. This could easily give rise to a large dollar amount of subsequent returns, which could result in significant losses for the financial institution if it is unable to successfully charge them back to the customer. More broadly, lack of monitoring could allow multiple customers to perpetrate a new type of fraud on a large scale for an extended period, multiplying the financial institution's exposure to ACH return-item losses. … Because of its important role, the monitoring of ACH consumer debit returns is already a well established risk-control practice. Indeed, rates of return are monitored routinely by credit card associations (in the case of credit cards) and NACHA (in the case of electronic funds transfers).

67. In 2006, the Office of the Comptroller of the Currency directed that national banks should report ACH return rate information to their boards of directors. *Automated Clearing House Activities: Risk Management Guidance*, OCC Bulletin 2006-39. The guidance stressed that ACH transactions involving certain high-risk originators (including telemarketers) or that involve third-party senders face increased reputation, credit, transaction, and compliance risks. Thus, banks that engage in high-risk ACH activities (i.e. deal with Third-Party Senders and originators such as telemarketers) should have strong systems to monitor and control risk.

68. The ACH system allows Receivers, and their Receiver Depositary Financial Institution, to return entries for a variety of reasons. The ACH system uses codes to identify the reason for returned transactions. The return codes include several for transactions that are unauthorized. The NACHA Operating Rules require that a bank returning an ACH transaction as unauthorized obtain a Written Statement Under Penalty

of Perjury from the consumer prior to returning the entry. High rates of ACH entries returned as unauthorized, or for other reasons such as insufficient funds and uncollected funds, serve as notice that the Originator is engaging in fraudulent practices.

69. The reasons for returns, as well as the nature of the underlying payment, are also relevant to fraud analysis. The ability to track ACH activity by Standard Entry Class (SEC) Code and by Return Reason Code enables identification of problem Originators, providing a critical risk mitigation tool to financial institutions that originate ACH transactions. ACH TEL transactions are particularly susceptible to fraud.

70. The monitoring obligation imposed includes not only the monitoring of the returns (and the reasons for the returns), but the monitoring of the original codes used for the ACH entry to assure they are not being misused. As part of the due diligence required in the underwriting of customers, a new originator should be approved for specific SEC codes reflecting their business practices. The choice of which ACH entry to use is determined by how the authorization to initiate the entry was or will be obtained. An originator approved for multiple codes will determine for each entry which code to use and submit it to the ODFI. This puts the legal responsibility on banks to assure that the correct coding is used, as an ODFI warrants that each entry it transmits is in accordance with proper authorization provided by the Originator and the Receiver. 2007 Operating Rule 2.2.1.1.

71. The 2002 NACHA Operations Bulletin noted that telemarketers, who frequently use TEL entries to process payment, often misuse the TEL entry and engage in unfair and deceptive trade practices. Those practices include acting with fraudulent intent to debit consumer accounts without authorization; cold-calling customers with

whom they have no previous relationship and manipulating the TEL rules by using mail solicitations to induce customers to initiate the call to the telemarketer and then sell their wares with deceptive practices.

72. The Operations Bulletin specifically recognized the fact that high return rates were a good indication of fraud in TEL transactions:

> It has become obvious that there is a correlation between high return rates relating to unauthorized debits and Originators that are violating the rules or that are engaged in fraudulent/deceptive marketing practices. These merchants are experiencing a volume of unauthorized returns in excess of the average for other unauthorized debit entries.

73. The 2008 NACHA Guidelines emphasize the interrelationship of fraud and high return rates, as well as the responsibility of ODFIs to address that fraud:

> A correlation has been established between high return rates relating to unauthorized debits and Originators that are violating the *NACHA Operating Rules* or are engaged in fraudulent/deceptive marketing practices. Such merchants typically experience a volume of unauthorized returns in excess of the average for unauthorized returns.

2008 Operating Guidelines 242.

74. Despite the existence of discreet coding for different types of returns, there is no guarantee that the return entry code accurately reflects the reason for the return. For example, a customer whose account has been subject to repetitive, unauthorized debits may close the account (resulting in an R02 return) or the successive debits may result in a return because the account is overdrawn. Furthermore, as noted above, many low value, fraudulent debits go undiscovered by the consumer victim; alternatively, the consumer who has been duped may be embarrassed at his or her vulnerability or may encounter roadblocks in attempting to achieve redress, so that a focus only on return rates may not reveal the entire extent of fraudulent operations.

75. NACHA publishes average industry return rates, both for total returns and for returns for specific reasons. Because the majority of returns are originated by a small number of banks, a simple comparison of one bank's average to the national average (or mean) may be somewhat misleading, and again may lead to an underassessment of fraud. In a study done in 2006 of ACH return rates, it was demonstrated that the national mean return rate for all ODFIs with one hundred or more forward ACH entries was 1.6%. By contrast, the median return rate was 0.9% (almost half the mean). In other words, half of all banks had a return rate *under* 0.9%, and 75% had return rates *under* 1.8%. Thus, having an "average" return rate means that a bank is *above the median* rate of return. Having a return rate just "slightly above" average (e.g. 1.8%) put the bank's returns in the top quartile and makes its return rates suspicious.

76. Despite these caveats, monitoring of return rates is a critical risk management tool. The Electronic Payments Network (EPN), the leading private ACH Operator, identified monitoring of ACH returns as one of its six recommended ACH risk management tools. *See* Armantier, *et. al.* at 5. Studies have shown that when the ACH system transitioned from a system primarily for recurring, regularized payments to a vehicle for one-time, non-recurring entries such as TEL and WEB, return rates were initially quite high. With monitoring and other enhanced controls instituted by banks, however, those rates were cut by factors of 4 (for TEL) and 8 (for WEB) between 2002 and 2004. Karen Furst and Daniel E. Nolle, *What's Your Risk with the Growing Use of ACH Payments?* Office of the Comptroller of the Currency *Quarterly Journal*, vol. 24. no. 4 (December): 21-43. Thus, it is possible for a bank to cut return rates, and curtail fraud, through monitoring of return rates and enhanced controls.

The Evidence of Zions' Knowledge of Fraudulent ACH Activity

77. Based on my review of the evidence in this case, I conclude that Zions was in possession of sufficient facts from which, as a banking institution, it had to have known that there was fraudulent activity taking place utilizing ACH entries initiated through Modern Payments, but that Zions turned a blind eye and failed to take corrective action to root out that fraudulent activity. First, the excessively high rates of returns generated by Modern Payments and its clients, of which Zions was well aware, cannot be tolerated within normal business models and are clear indications of fraud. Second, Zions knew that Modern Payments and many of its customers were "High Risk" clients with whom Zions should not be doing business. Third, Zions knew that inadequate due diligence had taken place in the underwriting of new high risk clients by Modern Payments and by Zions, and in their monitoring the activities of those customers. Last, Zions knew that it had itself engaged in, innumerable knowing violations of the NACHA rules on behalf of the Telemarketers in the authorization of and processing of ACH entries. All of these conclusions are based on evidence that is common to all the victims.

Excessively High Return Rates

78. The most glaring indication of fraudulent activity is the excessively high rates of returns generated by Modern Payments and its customers. Modern Payments started to process through Zions in September 2006. As discussed above, the overwhelming number of banks in the United States have no unauthorized returns at all. Zions' number of unauthorized returns immediately began to increase dramatically from *zero* in August 2006 to 799 in October, 2,095 to 2,632 by February 2007. By July 2007, Zions was *fourth* worst in the country in terms of unauthorized returns. However, when

the number of returns is adjusted for bank size, Zions was apparently the worst. The number and volume of total returns similarly skyrocketed. PA-268[4]; Fox Deposition at 85, 92, 94. Second, all the unauthorized returns were attributable to one source: Modern Payments. Third, legitimate businesses cannot tolerate such high return rates for both unauthorized and total returns over such periods. Anyone in possession of these facts would have to have known fraud was involved.

79. According to NACHA, in the year 2007 return rates for ACH debits were low, and unauthorized return rates had indeed declined (2007 ACH Network Statistics (PA-50)):

- Total return rate for ACH debits: 1.94%
- Returns for insufficient funds or uncollected funds (NSF): 1.35%
- Returns as unauthorized (R05, R07, R10 and R29): 0.041% (compared to 0.045% in 2006).

80. During 2007, Modern Payments had 13 clients identified as "high risk" in Zions' own reports whose *unauthorized* return rates exceeded 2% (49 times the average) and over 20 whose *total* returns exceed 10% (5 times the average). Not only did these clients exceed the reporting thresholds and the NACHA 2007 averages, they drastically exceeded them. PA-615:

- NHS: total returns 22 to 29 times the average (42.06 to 56.27%); unauthorized return rates 132 to 280 times average (5.42 to 11.45%);

[4] "PA" indicates the page of the document in the overall appendix submitted by Plaintiff in Support of Class Certification.

- Low Pay: total returns 21 to 46 times average (40.16 to 89.69%); unauthorized returns 36 to 100 times average (1.48 to 4.14%);

- Group One: total returns 24 to 35 times average (46.81 to 67.58%); unauthorized returns 26 to 85 times average (1.09 to 3.5%);

- Vexeldale and Paydayloan Resource Center: total returns 28 to 31 times average (53.70 – 60.71%);

- Digitel / Platinum Benefit: total returns 14 to 29 times average (26.17 - 56.65%);

- Market Power Marketing: total returns 39 to 50 times average (76.6 - 96.33%); unauthorized 59 to 123 times average (2.42 - 5.06%)

- RX Smart: total returns 9 to 21 times average (17.53 - 41.59%) unauthorized returns 261 to 426 times average (10.70 - 17.45%).

81. These extraordinarily high rates of return continued into the first seven months of 2008. Zions had over 13 entities on its list of high risk clients with unauthorized return rates in excess of 1% and over 14 with total return rates in excess of 10%. Again, the degree by which these customers exceeded the national average for 2007 was astronomical:

- NHS: total returns 28 to 31 times the average (55.12 to 59.71%); unauthorized return rates 209 to 379 times average (8.6 to 15.53%);

- Low Pay: total returns 29 to 43 times average (55.96 to 83.33%); unauthorized returns 19 to 126 times average (0.77 to 5.16%);

- Group One: total returns 8 to 84 times average (16.22 to 163.41%); unauthorized returns 20 to 478 times average (0.8 to 19.59%);

- Digitel / Platinum Benefit: total returns 10 to 29 times average (20.19% - 56.65%); unauthorized returns 22 to 37 times average (0.89 – 1.53%);

- Market Power Marketing total returns 39 to 50 times average (76.6% - 96.33%); unauthorized 59 to 123 times average (2.42% - 5.06%).

82. It is obvious that the high rates of unauthorized returns are indicative of fraudulent activity by these companies. Since the overwhelming majority of banks in the United States have no unauthorized returns at all, anyone looking at the high over-all return rates (many over 50%) would know that legitimate businesses would not and could not go on with such high return rates for any reason. These are high return rates for clients transmitting more than 500 entries per month. Indeed these high rates of return are characteristic of businesses that do the ACH equivalent of "phishing" where they purchase lists of bank account numbers to utilize in the hopes that some of them are "good." They then do the equivalent of "slamming": rather than switching a consumer's phone service without permission, the company charges the consumer's bank account without permission. This is not done for simply one account; the entire list of "acquired" account numbers are entered *en masse* into the ACH system in the hopes that a few will prove to be valid. PA-363. In a society where lists of account numbers can be acquired in illegitimate ways, such activities are becoming a greater problem.

83. Viewing the data in the aggregate (rather than by Originator), also demonstrates that the depth of the problem was known to Zions. In August 2006, a month before Zions began processing payments for Modern Payments, it had no

unauthorized returns at all. Yet the NACHA reports of Fedwire returns during the time Modern Payments submitted ACH entries (from October 2, 2006 through the end of 2007) show a drastically changed picture: both the volume and dollar amount of returns (whether unauthorized or total returns are considered) began to skyrocket. (NACHA 05293 through 05510.) In the first two months of operation, the dollar value of total weekly returns *doubled* from $27,118.90 (week ending 10/06) to 54,406.0 (week ending 12/08). Within the next seven months (by the week ending 5/18/07), the total dollar value of returns had almost *quadrupled*, amounting to $107,308.03. By 7/13/07, the amount was up to $189,689.90. The number of returns for those same time periods went from 391 (10/06/07) to 1210 (7/13/07). (NACHA 01274.) While increase in volume may account for some of the dollar increase, it does not account for such a drastic increase as is present here.

84. The drastic increase can also be seen from the return entry reports of EPN (The Electronic Payments Network) on Originators with 200 or more unauthorized returns monthly, or 500 or more invalid account returns monthly. In February 2007, Zions has 587 unauthorized returns totaling $70,780.68, and 1942 invalid returns totaling $240,003.62. (NACHA 00237-00262; 00474-00557.) By November of 2007, nine months later, the number of unauthorized returns had more than trebled to 1877 totaling $168,556.85 and the number of invalid returns had more than doubled to 4182 totaling $192,506.88. (NACHA 00263-00343; 01274-01487.)

85. There is in the record only one possible cause for this dramatic increase. In August of 2006, Zions had no unauthorized returns. In September of 2006 Zions began processing payments for Modern Payments. In October, the drastic uptick in the

number of unauthorized returns (and the total number of returns) started. By December of 2006, Zions was aware that something was wrong in the ACH department, and an email was sent internally restating Zions' own ACH policy providing that internet and telephone initiated transaction are high risk and must be approved for processing "*only as an exception to policy*". PA-144.

86. Zions had other knowledge of glaring irregularities indicative of fraud gained from its knowledge of the returns. On the EPN reports, for example, many of the entries were in the same amounts for PPD entries, a sign of potential fraud. Additionally, many of the companies were not listed by name, but merely by a phone number (e.g. 866-xxx-xxxx) and initials; a quick web search of several of the recurring numbers brought up consumer complaints to such sites as "ripoffreport.com" or "complaintsboard.com."

87. These facts, when combined with some of the testimony in this case, lead to the inescapable conclusion that it would have been clear to any banker properly familiar with the regulatory requirements discussed above that fraudulent activity was present in the processing of Modern Payments entries.

Knowledge of High Risk Customers;
Lack of Due Diligence in On-Boarding and Monitoring of Activity

88. There is evidence establishing that Zions knew that it was originating ACH transactions for high risk customers who were on-boarded or brought on as customers without the necessary due diligence in assessing their businesses and without the necessary due diligence in the monitoring of their operations.

89. As early as November 2006, in a key meeting attended by Zions executive Danne Buchanan, the high risk nature of Modern Payments's client base was discussed in the context of OCC Bulletin 2006-39 emphasizing that ODFIs like Zions were legally responsible for the actions of Third-Party Senders (Modern Payments) and their customers. PA-158. Also in November 2006, Zions was contacted by Jeanette Fox of NACHA who alerted Zions that a number of Modern Payments' originators were on NACHA's "watch list" and that she was surprised to see that Zions was doing business with them. PA-201. The email by a Zions employee recounting the discussion with Fox states that Zions had legal responsibility for Modern Payments' entries but was not aware of the due diligence being undertaken. In January of 2007, in an email to Danne Buchanan, Steve Houston, Executive Vice President of Zions, noted that of a client sample he had been sent of Modern Payments' customers, there were business types the "we would not allow at the bank level for either debit or credit ACH risk." Indeed, speaking generally of the client samples he had seen, he noted "Typically, our Banks would avoid debit ACH relationships with these companies unless they were well known and very well-established in our local market." PA-78. Houston recognized the "staggering" nature of Modern Payments' return rates. Despite this knowledge of the troubled nature of these ACH Originators with whom Zions was acting as the ODFI, Zions continued to do business with them and Modern Payments, apparently under the rationale (articulated in Houston's email) that through an appropriate pricing model the various risks to the bank could be accommodated.

90. The Houston email also pointed out the lack of due diligence in the underwriting of new customers, which he called "cursory at best." Deficiencies noted by

Houston included failure to do due diligence on the principals of a company; failure to take action when the bona fides of a principal could not be verified; failure to check bank references; and the failure to assure that some of these business lines, which "could well be used for money laundering purposes" did not present any risks. He further noted the lack of any risk management policies and procedures. PA- 78. Additionally, the individuals responsible for the "due diligence" or the underwriting of new customers for Modern Payments had received no training in what to look for or how to evaluate new customers who would be allowed to originate ACH transactions. Deposition of Melinda Whiting p. 19, l. 4, PA-563. As late as October, 2007 Zions was well aware that "there isn't anyone within [Modern Payments] that has credit experience to properly evaluate and approve new clients." PA-100.

91. In March of 2007, an Internal Audit Report was done of Modern Payments, a wholly owned subsidiary of Zions Bancorporation. The overall conclusion: an ***Unsatisfactory*** rating. In particular, the report noted that the controls are "insufficient for a department within a regulated financial institution interacting with bank commercial customers." PA-273.

92. This evidence demonstrates that Zions was well aware of the high risk nature of the Telemarketer customers of Modern Payments and of the risks it took in dealing with them. When in January 2007 the FTC alerted Zions to the fact it was investigating several of Modern Payments' customers, Zions executive Danne Buchannan remarked that "This is exactly what I was afraid of." PA-80. Despite the warning that Modern Payments' controls were "insufficient for a department within a regulated financial institution," Zions continued to allow Modern Payments access to the ACH

system and to process payments on its behalf. As its business increased month after month, so did the exposure to risk and fraud.

93. It is also apparent what motivated Zions and Modern Payments to continue to do business with these high risk companies. An interoffice memorandum to the Chief credit officers, Steve Houston, Executive VP at Zions and Jerry Dent, Executive VP at Zions Bancorporation, noted that the main protection against these high risks was the maintenance of reserves: "I wonder why we involve ourselves with these High Risk clients given the possible credit risk and reputation risk they represent....When I queried about their philosophy behind doing the High Risk clients, I was told that the profit from these customers was needed to make the overall business profitable." PA-99-100. While Zions was concerned about profit, it does not appear to have been concerned about those victimized by fraudulent activity.

94. While Zions knew it was dealing with high risk customers, it also knew that the due diligence required in the underwriting or on-boarding of those customers was non-existent or cursory. The 2007 Audit (if nothing else) alerted them to the fact that the underwriting was inadequate. Several "Underwriting Score Templates" document that Modern Payments was making underwriting decisions on high risk customers with little or no information. For example, the Underwriting Score Templates for Vexeldale, ZFNB0003663, and Sourdale, ZFNB0003362, show that Lexis Nexis rated the risk of these businesses (both owned by the same individual) as high, but shows that in many areas there was no information to verify the company's credit scores, the individual's credit scores ("too many inquiries within past 12 months"), the existence of the companies, or any link between the authorized representative and the companies. Despite

these deficiencies, each company was approved on the basis of transactions amounting to $1.525M per month and $400K per month respectively. As a memo to a Zions Executive VP noted, "the credit files I reviewed lacked adequate documentation of [MP's] relationship with the client…One specific file (NHS) was deplete of information and the credit scores didn't support our doing business with them." ZFNB0002893.

95. Had Zions even looked at the applications it received, let alone done the necessary due diligence, it would have discovered, for example, that some of the clients of Modern Payments – indeed, those clients that established themselves as "high risk" clients – had a presence outside the United States. For example, NHS's application shows its president and authorized officer was located in Freeport, Bahamas even though the business was supposedly located in Collegeville, PA. MP 3.

96. There is also evidence in the record that as late as 2009 most of Modern Payments customers lacked appropriate underwriting. Digitel Network became a customer in 2006. In 2009 it was identified as a "high risk client not previously underwritten" in a "Due Diligence Risk Review." ZFNB0095677. An initial draft of the review concluded that because Modern Payments never had any trouble collecting processing fees or collecting funds from unauthorized returns previously paid out, no reserve was going to be required. That conclusion was edited to note that return rates were high and increasing, and that there was a question as to whether the authorizations being obtained were sufficient in disclosing that there would be recurring monthly charges to the consumer's account. ZFNB0102270.

97. In essence, the underwriting and due diligence that took place was tantamount to no underwriting at all. Zions was giving originators access to the entire

ACH system without performing basic required due diligence. Despite a policy that these customers should not have been accepted as ACH originators, despite knowledge that these were high risk clients, and despite statements of Zion executive Buchanan that the bank should not remain associated with these customers, the bank continued to process payments for them and the high return rates continued. PA-359; Fox Deposition at 121. In doing business with Modern Payments and its clients without the requisite due diligence in the onboarding of the customers and in the monitoring of their activities, Zions was knowingly departing from the guidance provided by its regulators, including but not limited to the Office of the Comptroller of the Currency and the Federal Financial Institutions Examination Council.

NACHA Rules Violations

98. Zions also knowingly engaged in violations of NACHA Rules (and its activity was also not in accordance with reasonable commercial standards of fair dealing). Its knowledge of Modern Payments' failure to abide by those rules, as well as its own failure to do so, are additional facts on which a finding of knowledge of fraud can be predicated. As the ODFI at the point of entry into the ACH system, Zions had an affirmative obligation to assure that all the protections inherent in the ACH system were being employed, and that the system was being used property.

99. Zions was clearly aware that Modern Payments' customers were improperly using ACH codes indicating the type of entry being initiated, in particular, the PPD and TEL codes, and that there was a history of such misuse. During 2006 and the first seven months of 2007, all Modern Payments entries were entered as PPD by Zions. In processing entries with that coding, Zions, as the ODFI, warranted that consumer debit

authorizations had been obtained in *pre-existing, signed writings* as required by both the NACHA rules and the Electronic Funds Transfers Act, 15. U.S.C. § 1693e(a). Yet Zions knew that this representation was false.

100. In December of 2006, Zions contacted Modern Payments to alert them that all of their transactions (which were then coded PPD) were, "understanding the types of businesses they are," more likely TEL or WEB transactions. Despite this recognition that the wrong SEC code was being used, Zions executive Danne Buchanan knew that the matter had not been corrected by February of 2007, although he was asked that it be done "as soon as possible." ZFNB0004543-4. Eight months later, October 2007, the transition in the use of SEC codes had yet to be completed. ZFNB0049725.

101. When Zions began to use other SEC codes beginning in late July of 2007, it engaged in similarly fraudulent activity. It began entering transactions derived from outbound telemarketing under the TEL code even though such transactions were explicitly forbidden from the ACH Network. After it began using the TEL code for such transactions it was quickly alerted by another bank, USAA Bank, from which it sought to debit funds that it was misusing the TEL code for outbound telemarketing transactions. As in its use of the PPD code, the use of the TEL code involved misrepresentation of warranties to the consumers' banks from which funds were being debited. Despite being advised of the use of improper codes Zions continued to attach the false codes and continued to misrepresent the warranties.

102. In accepting and transmitting entries which it knew were miscoded, and not based on the authorizations required by the NACHA rules and by federal statute,

Zions was in breach of its own warranties and was knowingly transmitting unauthorized and prohibited entries through the ACH system. Specifically, it was:

- Knowingly transmitting PPD entries that lacked the pre-existing, signed written authorization required by NACHA Operating Rules and federal law;
- Knowingly transmitting TEL entries for out-bound transactions that are prohibited by NACHA operating rules adopted to prevent fraudulent telemarketing; and
- Knowingly transmitting WEB entries for which the appropriate authorization had not been obtained.

103. Furthermore, Zions knowingly allowed Modern Payments to migrate from the use of PPD to WEB and TEL when such a migration evidences utilization of the ACH system in inappropriate ways to cover up the true nature of the underlying transactions. It allowed the migration to TEL knowing that Modern Payments customers were engaged in prohibited outbound-telemarketing in violation of the rules. When that abuse of the ACH system was discovered, the response was to suggest that Modern Payments and its clients switch to using remotely created checks that cleared differently. According to Casey Leloux, "A lot of our revenue is generated by clients with over 1% unauthorized returns. Turning them off or sending them somewhere else is not an option." PA-101. Zions was a knowing party in facilitating Modern Payments' clients who had been terminated.

104. In February, 2008 Casey Leloux of Modern Payments sent reference letters to Teledraft on behalf of NHS and Vexeldale in which he suggested that Teledraft

begin processing these companies using remotely created checks rather than ACH transactions. PA-478; PA-479. Since remotely created checks were more expensive and less efficient to transact than ACH transactions, I know of no reason why Leloux would have suggested to transfer the customers from ACH transactions to remotely created checks other than to have concealed the fraudulent behavior. Remotely created checks were less strictly monitored by regulators than were ACH transactions.

105. A second major violation of the NACHA rules of which Zions was aware of was its failure to enter into the required contract with the Third-Party Sender, Modern Payments. The main documentation of such an agreement identified by Zions' counsel establishing their relationship is a partially filled out application dated September 13, 2005 (ZFNB0002365). This is not the requisite contract and lacks the requisite warranties. The establishment of a legal relationship between the ODFI and the Third-Party Sender is essential to the integrity of the ACH system, allowing for the assertion of rights in the event of loss. Moreover, while not formally "required," it is strongly urged, and it is good business practice, for there to be agreements between the ODFI and the originators themselves. Again, these are lacking.

106. In processing payments for Modern Payments without a contract, Zions was knowingly breaching the following warranties:

- It knowingly violating the requirement that it enter into an agreement under which the Third-Party Sender agree to be bound by NACHA rules, agree to use the system only for lawful purposes, and agree to assume the responsibilities of an Originator.

- It knowingly breached its warranty that it had in place established procedures to monitor the Third-Party Sender and the originators.

- It knew that the Modern Payments had not made the warranties required under the NACHA Operating Rules.

107. In conclusion, Zions as an ODFI had a responsibility to guard access to the ACH system to prevent fraud. I conclude, however, that it knowingly allowed the system to be used by High Risk originators whom it had to know were engaged in fraud in clear disregard of the governing rules and standards, that it made knowing misrepresentations to the other participants in the ACH system (including the consumer receivers), that it facilitated the misuse of the system by Modern Payments and its customers, and it did all this knowing of facts from which, as a banking institution, it had to know fraud was taking place. As is clear from the above, the evidence establishing these conclusions will be common to virtually all the members of the class.

I hold the opinions expressed in this report to the reasonable degree of certainty applied by experts in my field.

I declare the above to be true under penalty of perjury.

 Dated: N Member 19, 2012

Amelia Helen Boss

AMELIA HELEN BOSS

Drexel University Earle Mack School of Law
3320 Market Street
Philadelphia PA 19104
215-571-4806
aboss@drexel.edu

BAR ADMISSIONS

New Jersey; Pennsylvania; United States District Court for the Eastern District of New Jersey; United States District Court for the Eastern District of Pennsylvania; United States Court of Appeals for the Third Circuit; United States Supreme Court

EDUCATION

Rutgers University School of Law, Camden, NJ
Juris Doctor, 1975. Honors and Activities: Degree Summa Cum Laude; Law Review; Dean's List, all semesters; Teaching Assistant (Contracts and Constitutional Law); Jessup International Moot Court

Bryn Mawr College, Bryn Mawr, PA
B. A. in Sociology, 1970. Honors: Degree Cum Laude; Honors in major

Foreign Study: University of Massachusetts Program, St. Hilda's College, Oxford University, England 1968

EMPLOYMENT

Teaching (courses taught: contracts, sales, payments systems, secured transactions, bankruptcy, international business transactions, international commercial transactions)

2008-present: Trustee Professor of Law, Drexel University Earle Mack School of Law, Philadelphia PA

Summer 2010: Summer Program, Law College of England and Wales, London; University of San Diego Law

1989-2008: Professor of Law, Temple University School of Law, Philadelphia, PA (Charles Klein Professor of Law 1999-2002, Associate Professor 1989-92)

Spring 2005: Temple University Law School LL.M Program, Beijing, China

Fall 2004: Visiting Professor of Law, Victoria University of Wellington, New Zealand

Spring 1998: Leo Goodwin Distinguished Visiting Professor of Law, Nova Southeastern University School of Law, FL

Summer 1998: Temple University Law School Summer Program, Athens, Greece

Summer 1996: Temple University Law School Summer Program, Rome, Italy

Spring 1994: Temple University Law School, Semester Program, Tokyo, Japan

Summer 1987: Summer Program, Trinity College, Dublin, Ireland; University of San Diego School of Law

1983-1987: Associate Professor (Assistant Professor 1978-83); Rutgers University School of Law, Camden, NJ

1985-1986: Visiting Professor of Law; University of Miami School of Law, Coral Gables, FL

Other Legal Experience

1987-1989: McCarter & English, Cherry Hill, NJ

1976-1978: Pepper, Hamilton & Scheetz, Philadelphia, PA

1975-1976: Law Clerk, Honorable Milton B. Conford, Supreme Court of New Jersey

PUBLICATIONS

Convergence in Electronic Banking: Technological Convergence, Systems Convergence, Legal Convergence, 1 DREXEL LAW REVIEW 63 (2009); *also published in*, DERECHO DEL SISTEMA FINANCIERO Y TECNOLOGÍA (Augustin Madrid Parra, ed. 2010).

The Evolution of Commercial Law Norms: Lessons to be Learned from Electronic Commerce, 34 BROOKLYN JOURNAL OF INTERNATIONAL LAW 673 (2009)

THE UNITED NATIONS CONVENTION ON THE USE OF ELECTRONIC COMMUNICATIONS IN INTERNATIONAL CONTRACTS: AN IN-DEPTH GUIDE AND ANALYSIS (with W. Kilian, eds) (Kluwer Law International 2008)

Becoming Operational: Electronic Registries and Transfer of Rights, in UNCITRAL CONGRESS ON MODEL LAW FOR GLOBAL COMMERCE (United Nations 2008)

The Honorable Dolores Sloviter: An Oral History, in WOMEN TRAILBLAZERS IN THE LAW: OUR VISIONS, OUR VOICES (ABA Commission on Women in the Profession 2007)

The Future of the Uniform Commercial Code in an Increasingly International World, 68 OHIO STATE LAW JOURNAL 349 (2007)

The U.S.-China Roundtables: Fostering Cross-Cultural Dialogue and Scholarship, 24 TEMPLE JOURNAL OF SCIENCE TECHNOLOGY AND ENVIRONMENTAL LAW 219 (2005) (with Jeffrey L. Dunoff)

Cyberspace Exploration under the New Zealand Electronic Transactions Act 2002: A Review of Bob Dugan and Ben Dugan, ELECTRONIC TRANSACTIONS, 21 NEW ZEALAND UNIVERSITIES LAW REVIEW (2005)

ABCS OF THE UCC: ARTICLE 2A LEASING (Second Edition, ABA 2005) (with S. Whelan)

Does the Conclusion of Contract by Electronic Means Change the Grounds of the Notion of Contract, in LES DEUXIÈMES JOURNÉES INTERNATIONALES DU DROIT DU COMMERCE ÉLECTRONIQUE. LE CONTRAT ÉLECTRONIQUE, LITEC, BIBLIOTHÈQUE DU DROIT DE L'ENTREPRISE, (Eric Caprioli, ed., 2004)

Regime Juridique du Contract Conclu Par Voie Electronique: Quelques Apports de Common Law, LE JOURNAL DES SOCIETÉS (2004)

Electronic Contracting: Legal Problem or Legal Solution, in HARMONIZED DEVELOPMENT OF LEGAL AND REGULATORY SYSTEMS FOR ELECTRONIC COMMERCE IN ASIA AND THE PACIFIC: CURRENT CHALLENGES AND CAPACITY BUILDING NEEDS (United Nations Economic and Social Commission for Asia and the Pacific 2004)

ELECTRONIC COMMERCE: TRAINFORTRADE MATERIALS (United Nations Commission on Trade and Development 2002) (author and editor)

Taking UCITA on the Road: What Lessons Have We Learned?, 7 ROGER WILLIAMS LAW REVIEW 167-213 (2001), *earlier version in* UNIFORM COMPUTER TRANSACTIONS ACT: A BROAD PERSPECTIVE (Practising Law Institute 2001).

The Uniform Electronic Transactions Act in a Global Environment, 37 IDAHO LAW REVIEW 275-342 (2001)

Searching for Security in the Law of Electronic Commerce, 23 NOVA LAW REVIEW 585 (Winter 1999)

Legal Dimensions of Electronic Commerce, Report prepared for the United Nations Commission on Trade and Development, TD/B/COM.3/EM.8/2, (May 1999)

The Jurisdiction of Commercial Law: Party Autonomy in Choosing Applicable Law and Forum under Proposed Revisions to the Uniform Commercial Code, 32 INTERNATIONAL LAWYER 1067 (Winter 1998)

Electronic Commerce and the Symbiotic Relationship Between International and Domestic Law Reform, 72 TULANE LAW REVIEW 1931 (1998)

ABCs OF THE UCC: ARTICLE 5 LETTERS OF CREDIT (ABA 1998) (with J. Barnes and J. Byrne)

The Emerging Law of International Electronic Commerce, 52 BUSINESS LAWYER 1469 (1997) (with J. Winn)

ABCs OF THE UCC: ARTICLE 2A LEASING (ABA 1997) (with S. Whelan)

Consumer Transactions and the Code: Some Considerations, 51 BUSINESS LAWYER 1343-1360 (1996) (with K. Patchel)

Statutory Treatment of Leasing Transactions: The Legislative History of Article 2A and the UNIDROIT Convention on International Financial Leasing, Chapter 2 *in* 1 EQUIPMENT LEASING (Jeffrey J. Wong, ed.) (1995)

Book Review, 1 EDI LAW REVIEW 299 (1994) (reviewing Walden and Braganza, EDI: AUDIT AND CONTROL and Marcella and Chan, EDI SECURITY, CONTROL AND AUDIT)

The Legal Status of Electronic Data Interchange in the United States, in ELECTRONIC DATA INTERCHANGE (EDI): AUS ÖKONOMISCHER UND JURISTISCHER SICHT (W. Kilian, et. al) (Nomos Verlagsgesellschaft 1994)

Is the UCC Dead, Alive or Well? An Introduction to the Practitioner's Perspective, 12 LOYOLA OF LOS ANGELES LAW REVIEW 1901 (1994)

The Impact of Fiscal Recordkeeping Requirements on the Migration Towards Electronic Technologies: The United States Experience, 1 THE EDI LAW REVIEW 175-193 (1994) (with M. Decastro)

ELECTRONIC DATA INTERCHANGE AGREEMENTS: A GUIDE AND SOURCE BOOK (International Chamber of Commerce 1993) (with J. Ritter)

Suretyship and Letters of Credit: Subrogation Revisited, 34 WILLIAM & MARY LAW REVIEW 1087 (1993)

Introduction to the Uniform Commercial Code Survey: A Plea for Cooperation, 48 BUSINESS LAWYER 1583-1594 (1993) (with S. Veltri)

A Legislative Response to the Issues of Software Contracting, COMMERCIAL LAW ANNUAL 27-86 (1993) (with J. Ritter)

Introducing the New Article 2A: Leases, 17 ALI-ABA COURSE MATERIALS JOURNAL 37 (1993)

The Emerging Law of International Electronic Commerce, 6 TEMPLE INTERNATIONAL AND COMPARATIVE LAW JOURNAL 293-309 (1992)

Divergent or Parallel Tracks: International and Domestic Codification of Commercial Law, 47 BUSINESS LAWYER 1505-1515 (1992) (with P. Fry)

THE LEGAL STATUS OF ELECTRONIC DATA INTERCHANGE IN THE UNITED STATES (ELTRADO Project, 1992)

Electronic Data Interchange Agreements: Private Contract Towards a Global Environment, 13 NORTHWESTERN JOURNAL OF INTERNATIONAL LAW AND BUSINESS 31-70 (1992)

A Legislative Response to the Issues of Software Procurement: A Report on the American Experience, in NORDIC YEARBOOK OF LAW AND INFORMATICS 62 (1992)

Real Estate in Bankruptcy: Avoiding the Trustee's Avoidance Powers Part II - Lease Terminations, 1 JOURNAL OF BANKRUPTCY LAW AND PRACTICE 286-303 (1992)

Real Estate in Bankruptcy: Avoiding the Trustee's Avoidance Powers Part I - Foreclosures, 1 JOURNAL OF BANKRUPTCY LAW AND PRACTICE 150-179 (1992)

The International Commercial Use of Electronic Data Interchange and Electronic Communications Technologies, 46 BUSINESS LAWYER 1787-1802 (1991)

Developments on the Fringe: Article 2 Revisions, Computer Contracting and Suretyship, 46 BUSINESS LAWYER 1803-1821 (1991)

International Commercial Practices, *in* INTERNATIONAL LAW (Ohio CLE Institute, 1991)

Bringing Suretyship into the Twenty-First Century: ALI to Draft a Restatement of Suretyship, 11 BUSINESS LAWYER UPDATE (March/April 1991), *reprinted in* REAL ESTATE DEFAULTS, WORKOUTS AND REORGANIZATIONS (ALI-ABA 1991)

Article 2A: Leases – Everything Your Need to Know But Haven't Had Time to Learn (With Bibliography), in EQUIPMENT LEASING (Commercial Law League of America Fund for Public Education, 1991)

The UNIDROIT Convention on International Financial Leasing, paper presented at program entitled Internationalization of Commercial Law (ABA Annual Meeting, August, 1990)

The Legislative History of Article 2A Revisited, *in* 1991 COMMERCIAL LAW ANNUAL 205-255

The Commercial Use of Electronic Data Interchange: A Report, 45 BUSINESS LAWYER 1645-1716 (1990) (with J. Ritter)

The Model Form of Electronic Data Interchange Trading Partner Agreement and Commentary (American Bar Association 1989) (with M. Baum, T. McCarthy, P. Otero and J. Ritter), *republished in* 45 BUSINESS LAWYER 1717-1749 (1990)

Warranty Provisions; Finance Leases; Consumer Leases, in BASIC UCC SKILLS: ARTICLE 2A (Practicing Law Institute 1990)

Report on the UNIDROIT Convention on International Financial Leasing (A Report to the American Bar Association 1989) (principal author) (October 1989)

Commercial Law Aspects of Equipment Leasing, chapter in EQUIPMENT LEASING 1989 41-96 (Practicing Law Institute 1989) (with J. Wong)

Scope of the Uniform Commercial Code: Advances in Technology and Survey of Computer Contracting Cases, 44 BUSINESS LAWYER 1671-1698 (1989) (with H. Weinberg & W. Woodward)

True Lease or Secured Transaction: The New Definition of UCC Section 1-201(37), 44 CONSUMER LAW QUARTERLY REPORT 3-8 (1989)

Article 2A on Leases - An Introduction to the Statute, 2 THE CORPORATE ANALYST 1-35 (1989), published in an earlier version in EQUIPMENT LEASING 1989 (Practicing Law Institute 1989)

ELECTRONIC MESSAGING: A REPORT OF THE AD HOC SUBCOMMITTEE ON SCOPE OF THE UCC (American Bar Association 1989) (with M. Baum and P. Fry)

Priority Problems Involving Consignments under The Uniform Commercial Code: Recent Developments (Continuing Legal Education Satellite Network Inc. 1989)

Commercial Law Aspects of Equipment Leasing, Chapter 1 in EQUIPMENT LEASING 1988 (Practicing Law Institute 1988) (I. Shrank & W. Flowers, ed.)

The History of Article 2A: A Lesson for Practitioner and Scholar Alike, 39 ALABAMA LAW REVIEW 575-614 (1988) (symposium on Article 2A), reprinted in 1991 COMMERCIAL LAW ANNUAL

Scope of the Uniform Commercial Code; Survey of Computer Contracting Cases, 43 BUSINESS LAWYER 1513-1554 (August 1988) (with W. Woodward), *reprinted in* 10 COMPUTER LAW REPORTER 50-91 (1989)

REPORT OF THE INTERNATIONAL OBSERVER MISSION, PALAU REFERENDUM, DECEMBER 1986 (with R. Clark, E. Hammerich, S. Roff and D. Wright) (International League for Human Rights and Minority Rights Group, New York, 1987)

Recent Developments in Chattel Security Law – 1985: The United States, Canada and the World, Chapter 5C in P. COOGAN, W. HOGAN & D. VAGTS, SECURED TRANSACTIONS UNDER THE U.C.C., 1A UNIFORM COMMERCIAL CODE SERVICE (Matthew Bender) (1985) (with Peter Coogan)

Purchase Money Security Interests, Chapter 19 in P. Coogan, W. Hogan & D. Vagts, SECURED TRANSACTIONS UNDER THE U.C.C., 1B UNIFORM COMMERCIAL CODE SERVICE (Matthew Bender) (1984)

Panacea or Nightmare? Leases in Article 2, 1984 BOSTON UNIVERSITY LAW REVIEW 39-108, *reprinted in* 1985 CORPORATE COUNSEL'S ANNUAL 883-892

Leases and Sales: Ne'er or Where Shall the Twain Meet, 1983 ARIZONA STATE LAW JOURNAL 357-393 (1983)

Lease Chattel Paper: Unitary Treatment of A `Special' Kind of Commercial Specialty, 1983 DUKE LAW JOURNAL 69-115 (1983), *reprinted in* 1984 CORPORATE COUNSEL'S ANNUAL 903-949

Uniform Commercial Code Treatment for All Leases, Chapter 4.3 in P. Coogan, W. Hogan & D. Vagts, SECURED TRANSACTIONS UNDER THE U.C.C., 1 UNIFORM COMMERCIAL CODE SERVICE (Matthew Bender) (1983) (with Peter Coogan)

Could & Should True Leases Be Brought Within the Coverage of Article 9? in PERSONAL PROPERTY LEASING 15-35 (ALI-ABA, Invitational Symposium Conference Materials, February 1983) (with Peter Coogan)

Products Liability and International Leasing Transactions: The UNIDROIT Draft Convention, 1 JOURNAL OF PRODUCTS LAW 143-161 (1982)

Environmental Law: Threshold Determinations Under the National Environmental Policy Act of 1969, 5 RUTGERS-CAMDEN LAW JOURNAL 380-98 (1974)

OTHER PUBLICATIONS

Editor-in-Chief - THE BUSINESS LAWYER (1998 - 1999)

Editor-in-Chief - THE DATALAW REPORT (Clark Boardman Callaghan)(1993-1997)

Editorial Board - THE JOURNAL OF BANKRUPTCY POLICY AND LAW

Editorial Board - THE EDI LAW REVIEW

Editorial Board - THE BUSINESS LAWYER (1998 - 2005)

Editor - ABCs OF THE UCC (book series published by American Bar Association)

PROFESSIONAL ACTIVITIES

Governor - Board of Governors, American Bar Association (2009-2011) [Finance Committee; Non-Dues Revenue Committee (Chair 2010); Liaison to Section of Legal Education]

Member - Council, The American Law Institute; Member Executive Committee (2007 - present)

Member - Advisory Board, Commercial Law Center, Gonzaga University

Director - Institute for International Law and Public Policy, Temple University Beasley School of Law (2002-2008)

Member - Commission on Women in the Profession, American Bar Association (2003 - 2006)

Member - Standing Committee on Membership, American Bar Association (2007 - 2009) (BOG liaison 2009 2112)

Chair - Steering Committee, DirectWomen (2006-2007) (also co-founder); Advisory Committee (2008 -)

Chair-Elect-American Association of Law Schools Section on Commercial and Consumer Law (2008-2009)

Chair - Section of Business Law, American Bar Association; Chair (2000-2001); Immediate Past Chair (2001-2002); Chair-Elect (1999-2000); Vice-Chair (1998 - 1999); Secretary (1997-1998); Council (1995-1997)

Delegate- American Bar Association House of Delegates (2004 - present)

Chair - Section Officers Conference, American Bar Association (2001-2003)

Delegate- United Nations Commission on International Trade Law Working Group on International Electronic Commerce (representing United States)

Expert - United Nations Commission on International Trade Law (on electronic commerce issues)

Consultant - United Nations Commission on Trade and Development (on electronic commerce issues)

Correspondent UNIDROIT – Institute for the Unification of Private International Law (Rome)

Member - Executive Committee, American Bar Association Section Officers Conference (representing Section and Division Secretaries 1997-98; Vice-chairs 1998-1999; Chairs-elect 1999-2000; Chairs 2000-2001; Delegates 2005-2006); Chair, Fall SOC Conference Planning Committee (2000, 2001); Chair, SOC Technology Committee (1999-2001)

Member - Standing Committee on International Technical Legal Assistance Projects, American Bar Association (1999-2000)

Member - Asian Legal Initiatives Council, American Bar Association (2000 - 2003)

Member - Board of Governors' Committee on Strategic Planning, American Bar Association (2002-2004, 2005-)

Member - Board of Governors' Committee on Business Competitiveness, American Bar Association (2000-2004)

Member - Dean's Leadership Council, Rutgers University School of Law Camden

Chair - Awards Committee, Rutgers University School of Law Camden Alumnae Association

Member - Committee to Review Scholarly Papers for the 2002 Annual Meeting, American Association of Law Schools (2001-2002)

Chair - Uniform Commercial Code Committee, ABA Section of Business Law (1991-1995)

Member - Permanent Editorial Board, Uniform Commercial Code (formerly ABA Advisor/Liaison; currently member of PEB Executive Committee)

Member - Uniform Commercial Code Article 2 Drafting Committee (Sales)

Member - Uniform Commercial Code Article 2B Drafting Committee (Software Licensing)

Member - Uniform Commercial Code Article 1 Drafting Committee (General Provisions)

Member - ALI Ad Hoc Committees on Article 2, Article 2A, and Article 2B

Advisor - National Conference of Commissioners on Uniform State Laws, Uniform Electronic Transactions Act Drafting Committee (representing American Bar Association)

Trustee - Board of Trustees, Community Legal Services, Inc., Philadelphia (1991-1997)

Trustee - Board of Trustees, Institute of International Commercial Law

Member - Computer Advisory Committee, American Arbitration Association (1990-1992)

Convener- Technology Coordinating Group, American Bar Association (1990-1991)

Member - Members Consultative Group, ALI Restatement of Suretyship; ALI Restatement (Third) of the Law of Torts: Products Liability

Chair - Subcommittee on Scope of the UCC, Uniform Commercial Code Committee of ABA Section of Business Law (1985-1991)

Vice-Chair - Electronic Commercial Practices Subcommittee, Uniform Commercial Code Committee of ABA Section on Business Law (1989-1990)

Chair - Working Group on UNIDROIT Principles of International Commercial Contracts, ABA Business Law Section

Chair - Working Group on UNIDROIT Convention on International Financial Leasing, ABA Business Law Section

Consultant- Advisory Committee on Private International Law, United States State Department

Member - Board of Regents, American College of Commercial Financial Lawyers

Advisor - United States Delegation to the United Nations Working Party on the Facilitation of International Trade Procedures (March 1990)

Member - Uniform Commercial Code Article 2 Study Committee (appointed by Permanent Editorial Board to review Article 2 on Sales and make recommendations about possible amendments)

Member - American Bar Association; New Jersey State Bar Association; Camden County Bar Association; Commercial Law League of America; American Bankruptcy Institute; National Association of Women Lawyers; International Bar Association

HONORS AND AWARDS

Charles Klein Professor of Law (1999-2002); American Bar Association Cyberspace Law Excellence Award (2004); Philadelphia Bar Association Dennis Replansky Memorial Award (2000); Rutgers Law School Armitage Award for Outstanding Alumna (1999); Friel-Scanlon Faculty Scholarship Award, 1994; American Law Institute (elected 1981); Glasscutter Award, American Bar Association Section of Business Law (1995); Fellow, American Bar Foundation; American Law Institute (elected 1981); *National Law Journal*'s Fifty Most Influential Women Lawyers In

America (March 1998); *Philadelphia Legal Intelligencer's* Women of Influence (February 2001); Marquis Who's Who in America, Marquis Who's Who in American Law, Marquis Who's Who of American Women., Marquis Who's Who in the East; Marquis Who's Who in American Education; IBC's 2000 Outstanding Women of the 21st Century; Who's Who in the 21st Century (International Biography Centre)